APLIKASI ENKRIPSI SMS BERBASIS JAVA MENGGUNAKAN ALGORITMA RSA

Yanuar Asshidqi[1], Adiwijawa[2], Andrian Rakhmatsyah[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Perkembangan Teknologi Komunikasi berkembang sangat cepat. Hal ini didukung dengan perkembangan telepon seluler sebagai media yang tidak hanya sebagai pengirim atau penerima data suara, akan tetapi dapat berupa text, gambar. Salah satu fasilitas yang paling digemari dan mudah digunakan yakni Short Message Service (SMS). SMS yang bersifat penting sangat diharapkan dalam pengirimannya dapat dikirimkan dengan aman kepada penerima, akan tetapi dengan fasilitas sekarang sangat dimungkin informasi SMS dapat dibaca oleh pihak-pihak tertentu.

Oleh karena itu, diperlukan adanya suatu mekanisme yang dapat menjaga kerahasiaan pesan penting tersebut. Salah satu metode menjaga kerahasian pesan yakni algoritma RSA. Pada tugas akhir ini, penulis membuat suatu aplikasi enkripsi SMS pada handphone yang berbasis Java 2.0. Aplikasi enkripsi ini dianalisis dari waktu respon dan penggunaan memori serta keamanan pada enkripsi dan dekripsi pesan.

Dari hasil percobaan, algoritma RSA merupakan salah satu algoritma yang tepat untuk digunakan dalam proses enkripsi pada handphone. Tetapi, dalam hal ini penulis menekankan pada segi keamanan pesan yang dikirim dan tidak mempermasalahkan besar atau biaya SMS yang dikirimkan

Kata Kunci : SMS, RSA, Java, enkripsi, dekripsi

Abstract

Technology of telecomunication increase very fast. It supported by developing of handphone that used as media for not only be sender or receiver data sound, but also text, images. One of facility in handphone that most delighted people is Short Messages Service (SMS). SMS is very important is not only to send the data but also the data must have security to protect from another user who is not allowed.

Therefore, we must have a mecanism that can protect the security important message. One of the method is RSA algorithm. In this case, the writer make SMS encryption application in the handphone use Java 2.0. the encryption application is analyted from response time and used memori, also security in the encryption and decryption message.

From the experience, RSA algorithm is a good way to solve the encryption and decryption. But, the writer more concretate in security message which is sent, and not consider the cost of SMS.

Keywords : SMS, RSA, Java, encryption, decryption

1. Pendahuluan

1.1 Latar belakang

Keamanan suatu data merupakan suatu prioritas tertinggi bagi seseorang user yang datanya tidak ingin diketahui oleh orang lain tanpa ijin atau sepengetahuan orang yang memiliki data tersebut. Oleh karena itu, banyak orang berusaha untuk membuat suatu sistem keamanan data yang lebih baik lagi, sehingga sampai saat ini sangat banyak produk yang dihasilkan dalam mengamankan datanya. Apalagi, pada aplikasi seperti SMS yang digunakan pada teknologi GSM dan CDMA sangat rawan akan pencurian data oleh orang yang paham akan spesifikasi dan teknologi dasar SMS, Sehingga diperlukan adanya suatu pengamanan atau kerahasiaan pesan.

Salah satu metode yang digunakan untuk menjaga kerahasiaan data adalah kriptografi. Kriptografi merupakan seni atau ilmu untuk menjaga kerahasiaan pesan[5,6,7]. Di dalam kriptografi, terdapat proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu data asli (*plaintext*) ke dalam bentuk yang tidak dapat dibaca (*ciphertext*) dengan menggunakan suatu kunci. Dekripsi adalah proses mengubah data yang sudah dalam bentuk yang tidak dapat dibaca (*ciphertext*) menjadi dapat dibaca (*plaintext*) dengan menggunakan suatu kunci. Untuk dapat melakukan enkripsi dan dekripsi, dibutuhkan algoritma (*cipher*) dan kunci. Algoritma atau Chiper adalah suatu fungsi matematika dan kunci adalah sederetan bit, dimana keduanya digunakan untuk proses enkripsi dan dekripsi. Untuk kunci pun ada 2 tipe, yaitu: kunci simetri yang menggunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya; dan kunci asimetri yang menggunakan sepasang kunci yang berbeda (publik dan pribadi) untuk melakukan proses enkripsi dan dekripsinya [5,6,[7].

Algoritma kriptografi yang akan digunakan dalam tugas akhir ini yakni algoritma RSA. Algoritma RSA dijabarkan pada tahun 1977 oleh Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology, huruf **RSA** itu sendiri juga berasal dari inisial nama mereka (**R**ivest—**S**hamir—**A**dleman) [2,5,7]. Algoritma RSA merupakan algoritma kunci asimetri yang memungkinkan tingkat sekuritasnya tinggi karena Algoritma RSA mempunyai *public key* yang dapat diketahui secara umum dan private key yang hanya diketahui oleh user yang mengenkripsi serta tingkat kesulitan pemfaktoran bilangan non prima menjadi faktor primanya [2,5,7].

Pada tugas akhir ini dikembangkan aplikasi untuk mengamankan data yang akan dikirim melalui handphone dengan menambahkan fasilitas pengiriman data text (SMS) yang dienkripsi menggunakan algoritma RSA dengan menggunakan teknologi Java 2 Micro Edition (J2ME). J2ME merupakan salah satu teknologi Java yang memungkinkan mobile user dapat mengakses dan berinteraksi dengan informasi serta layanan-layanan aplikasi wireless, antara lain fasilitas security tambahan misalnya dengan cara mengenkripsi terhadap pesan yang akan dikirimkan sehingga diharapkan akan didapat suatu aplikasi pengiriman pesan terenkripsi yang cepat, lebih aman dan mudah untuk digunakan

sehingga data penting yang bersifat rahasia hanya dapat dibaca oleh orang yang dituju.

1.2 Perumusan masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana membuat suatu aplikasi enkripsi data SMS menggunakan algoritma RSA yang dapat digunakan pada handphone yang mensupport teknologi Java 2 Micro Edition (J2ME) .
2. Pemilihan algoritma RSA pada aplikasi enkripsi SMS karena menggunakan public key dan private key serta adanya tingkat sekuritas yang tinggi karena tingkat kesulitan pemfaktoran bilangan non prima menjadi faktor primanya untuk mendapatkan private key.

Ruang lingkup yang menjadi batasan masalah pada penelitian tugas akhir ini antara lain:

1. Antara pengirim dan penerima sms sudah mengetahui private key atau *bit key* yang digunakan dan berhak mengubahnya.
2. Pengenkripsian dan pendekripsian hanya bisa dilakukan jika aplikasi sedang dijalankan pada handphone.
3. Data yang akan dienkripsi dan didekripsi dititik beratkan pada masalah tingkat keamanan sms sehingga tidak mempermasalahkan masalah biaya yang dikenakan.

1.3 Tujuan

Tujuan dari penelitian tugas akhir ini adalah :

1. Mengimplementasikan algoritma kriptografi RSA ke dalam sebuah handphone yakni aplikasi SMS pada handphone dalam menerima maupun mengirim pesan dalam bentuk teks dengan penggunaan pengenkripsian data.
2. Menganalisa performansi (kecepatan, penggunaan memori, keamanan) algoritma kriptografi RSA terhadap aplikasi SMS yang dibangun pada handphone.

1.4 Metodologi penyelesaian masalah

Metodologi pembahasan yang digunakan dalam penelitian Tugas Akhir ini adalah:

1. Studi pustaka :
   a. Pencarian referensi
      Mencari referensi yang berhubungan dengan Kriptografi terutama untuk Algoritma RSA dan hal-hal yang berkaitan dengan arsitektur SMS (sistem kerja, format sms, dll) serta J2ME.
   b. Pendalaman materi
      Mempelajari dan memahami proses enkripsi dan deskripsi algoritma RSA, arsitektur sms pada handphone, serta bahasa pemrograman yang digunakan.

2. Perancangan Perangkat Lunak
   Perancangan Perangkat Lunak dengan menggunakan konsep analisis dan desain yang berorientasikan objek. Dalam hal ini, pemodelan yang akan digunakan adalah UML (*Unified Modeling Language*).
3. Pembangunan aplikasi
   Implementasi apliklasi yakni dengan menggunakan J2ME untuk pembangunan aplikasi sms baik enkripsi maupun deskripsi berdasarkan algoritma RSA dengan memperhatikan spesifikasi yang ingin dibuat.
4. Analisis hasil aplikasi
   Aplikasi yang telah dibangun akan dilakukan pengujian atau testing yakni berdasarkan penggunaan memori, kecepatan, keamanan. Setelah diuji, akan di analisis berdasarkan tingkat keamanan aplikasi sms tersebut .
5. Penyusunan laporan tugas akhir dan kesimpulan akhir.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Berdasarkan waktu yang digunakan untuk proses enkripsi dan dekripsi pesan, maka proses dekripsi baik menggunakan *bit key* 1024 bit maupun *bit key* 2048 bit membutuhkan waktu yang lebih lama dibandingkan dengan waktu yang digunakan pada proses enkripsi menggunakan *bit key* 1024 bit dan *bit key* 2048 bit dan kenaikannya membentuk kurva exponensial berdasarkan jumlah karakter yang dikirimkan.
2. Berdasarkan penggunaan bit key yang digunakan baik untuk proses enkripsi dan dekripsi pesan, penggunaan *bit key 2048* bit memakan waktu lebih lama dibandingkan dengan penggunaan *bit key* 1024 bit dan kenaikannya membentuk kurva exponensial berdasarkan jumlah karakter yang dikirimkan sehingga dapat disimpulkan semakin besar bit key yang digunakan akan semakin lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi.
3. Berdasarkan tingkat keamanannya, penggunaan *bit key 2048* bit lebih aman dibandingkan dengan penggunaan *bit key* 1024 bit karena sulitnya pemfaktoran nilai modulus(*n*) menjadi bilangan pemfaktornya yakni pada *bit key* 2048 bit mempunyai jumlah bilangan prima kurang dari n yang lebih besar dibandingkan dengan *bit key* 1024 bit, sehingga dapat disimpulkan semakin besar bit key yang digunakan maka semakin tinggi pula tingkat keamanannya.
4. Berdasarkan penggunaan memori yang dipakai dan jumlah SMS yang dikirimkan, penggunaan *bit key* 2048 bit memakai memori lebih besar dibandingkan dengan *bit key* 1024 bit maka semakin tinggi bit key yang dipakai dan jumlah karakter SMS yang dikirimkan akan semakin besar penggunaan memori yang dipakai.

5.2 Saran

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Aplikasi ini diharapkan dapat mengirim pesan menggunakan kontak nomor pada handphone untuk pengirim tujuan pesan.
2. Aplikasi ini diharapkan dapat membalas atau me-*reply* langsung pesan yang sudah diterima tanpa harus kembali ke menu utama seperti pada aplikasi SMS sekarang yang umum sudah digunakan.
3. Aplikasi ini diharapkan dapat menyimpan pesan yang telah dikirimkan sebagai arsip.

Daftar Pustaka

[1] Gunawan, Arief Hamdani. *Kriptografi: Suatu Pengantar*: http://www.Ristishop.com 22 Juli 2005, tanggal download: 15 Juli 2007

[2] http://en.wikipedia.org/wiki/RSA.htm, "RSA" tanggal download : 15 juli 2007

[3] http://pajhome.org.uk/crypt/rsa/index.html "Exploring RSA Encryption" tanggal download : 15 juli 2007

[4] http://www.forum.nokia.com, " A Brief Introduction to Secure SMS Messaging in MIDP" tanggal download : 15 September 2007

[5] Hartanto, Aditya Antonius, 2004 "Pemrograman Mobile Java dengan MIDP 2.0" Andi. Yogyakarta.

[6] Kurniawan, Yusuf. Ir.MT., 2004 "Kriptografi : Keamanan Internet dan Jaringan Komunikasi", Penerbit Informatika, Bandung.

[7] Munir, Rinaldi, 2002, "Diktat Matakuliah Kriptografi : Algoritma RSA dan ElGamal" ITB, Bandung.

[8] Raharjo, Budi dkk, 2007, "Tuntunan Pemrograman Java Untuk Handphone" Informatika. Bandung.

[9] Rahayu, Florensia S, 2005, "Suplemen Bahan Ajar Mata Kuliah proteksi dan Teknik Keamanan Sistem Informasi", Tugas Kriptografi Fakultas Ilmu Komputer Universitas Indonesia, Jakarta.

[10] Rivest, R.L, A.Shamir, L.Adleman, "Security of Method : Cryptanalytic Approach", Laboratory for Computer Science, Massachusetts Institute of Technology Cambridge.

[11] Tamici, Halga, 2007. "Tugas Keamanan Sistem Lanjut : Analisis Kerja Kriptografi", ITB, Bandung.